National Infrastructure Protection Center
CyberNotes

Issue #2000-21 *October 23, 2000*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between October 6 and October 19, 2000. The table provides the vendor/operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear as red and/or italic text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Apache[1] *Patch now available*[2]	**Apache versions 1.3.12 and prior**	**A vulnerability exists if a RewriteRule directive is expressed which could let a malicious user view arbitrary files.**	**A patch is currently being tested and will be part of the release of Apache 1.3.13. Until then, users should check their configuration files and not use rules that map to a filename.** *Apache 1.3.14 is available for download at:* http://httpd.apache.org/dist/	**Apache Rewrite Arbitrary File Disclosure**	**Medium/ High (High if network security best-practices not in place.)**	**Bug discussed in newsgroups and websites.**

[1] Securiteam, October 3, 2000.
[2] Bugtraq, October 13, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Bardon Data Systems[3] Windows 95/98/NT 4.0/2000	WinU 5.1 and previous	A built-in emergency password is contained in this tool, however a number of the passwords are publicly available which could let a malicious user to gain full administrative privileges.	No workaround or patch available at time of publishing.	WinU Backdoor Password	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
BB4 Technologies[4]	Big Brother Network Monitor 1.5c2	An improper filtering vulnerability exists when '&' characters are used, which could let malicious users run arbitrary shell commands.	Upgrade to 1.5c2 available at: http://bb4.com	Big Brother Arbitrary Shell Command Execution	**High**	Bug discussed in newsgroups and websites.
Bytes[5] Windows NT 4.0/2000, Unix	Interactive Web Shopper 1.0, 2.0	A directory traversal vulnerability exists which could let a remote malicious user gain read access to any known file.	No workaround or patch available at time of publishing.	Interactive Web Shopper Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
CGI Script Center[6] Windows 95/98/NT 4.0/2000, Unix	Auction Weaver LITE 1.0, 1.01-1.04	Multiple vulnerabilities exist which could allow a remote malicious user to create, read, or delete arbitrary files.	Upgrade to Auction Weaver 1.05 available at: http://www.cgiscriptcenter.com/awl/	Auction Weaver Multiple Vulnerabilities CVE name CAN-2000-0810 CAN-2000-0811	Medium	Bug discussed in newsgroups and websites.
Cisco[7] ***Patch has been issued[8]***	**PIX Firewall 4.2(5), 4.2.1, 4.2.2, 4.3, 4.4(4), 5.0-5.2**	**A vulnerability exists in the algorithm that is used to prevent usage of unwanted commands, which could let a malicious user bypass this protection.**	***Find details on the patch and advisory at:*** http://www.cisco.com/warp/public/707/PIXfirewallSMTPfilter-pub.shtml ***However, the patch itself is incomplete since it still allows issuing these commands, just not in an interactive mode.***	**Cisco PIX Firewall SMTP Content Filtering Evasion**	**Medium/ High (High if DDoS best practices not in place)**	**Bug discussed in newsgroups and websites. Exploit has been published.**
Daniel Stenberg[9] Unix	cURL prior to version 6.0-1.1; cURL-ssl prior to version 6.0-1.2; Debian GNU/Linux 2.2	A vulnerability exists in the code that logs errors, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://security.debian.org/dists/stable/updates/main/	cURL Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[3] Securiteam, October 16, 2000.
[4] Bugtraq, October 10, 2000.
[5] Bugtraq, October 8, 2000.
[6] eSecurityOnline.com, October 18, 2000.
[7] Bugtraq, September 19, 2000.
[8] Securiteam, October 9, 2000.
[9] Debian Security Advisory, Debian-00-33-1, October 14, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Debian[10] Unix	Boa Webserver 0.94.8.2x and earlier 0.94	A security vulnerability exists due to improper filtering of percent-encoded characters, which could allow a malicious user to access files outside the document root of the web server.	Upgrade available at: http://security.debian.org/dists/potato/updates/main The Boa development team has released v0.94.8.3 which fixes this vulnerability available at: http://www.boa.org	Boa Webserver File Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Evolvable Corporation[11] Windows 95/09/NT 4.0/2000	Shambala Server 4.5	Two vulnerabilities exists: a Denial of Service vulnerability; and a plaintext password storage vulnerability, which could let a malicious user gain full control over the server and possibly other services if the passwords have been reused.	The vulnerabilities will be fixed in the next release.	Shambala Server Denial of Service and Plaintext Password Storage	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
eXtropia[12] Windows NT 4.0/2000, Unix	WebStore 1.0, 2.0	A directory traversal vulnerability exists which could let a remote malicious user gain read access to any known file.	Upgrade to the latest version available at: http://www.extropia.com/download.html	WebStore Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
FreeBSD[13] Unix	FreeBSD 2.x, 3.x, 4.0-4.1.1	A weak authentication vulnerability exists which could let a remote malicious user elevate his/her privileges.	Patch available at: ftp://ftp.freebsd.org/pub/FreeBSD/CERT/patches/SA-00:52/tcp-iss.patch	FreeBSD Weak Initial Sequence Number	Medium	Bug discussed in newsgroups and websites.
FreeBSD[14] Unix	FreeBSD 4.1.1	A file disclosure vulnerability exists which could let a remote malicious user read arbitrary files on the system. This may disclose confidential information and may facilitate further attacks on the system.	Patch available at: ftp://ftp.freebsd.org/pub/FreeBSD/CERT/patches/SA-00:54/fingerd.patch	FreeBSD fingerd File Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
GnuPG[15]	GnuPG 1.0-1.0.3	A vulnerability exists that could allow a malicious user to modify a file signed with multiple signatures. This vulnerability could allow a message to be altered without the program detecting it.	Upgrade available at: ftp://ftp.guug.de/gcrypt/devel/gnupg-1.0.3b.tar.gz	GnuPG Multiple Signed Message Modification	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[10] Debian Security Advisory, October 9, 2000.
[11] Bugtraq, October 9, 2000.
[12] Bugtraq, October 9, 2000.
[13] FreeBSD, Inc. Security Advisory, FreeBSD-SA-00:52, October 6, 2000.
[14] FreeBSD Security Advisory, FreeBSD-SA-00:54, October 13, 2000.
[15] Bugtraq, October 13, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Hewlett-Packard[16]	JetDirect x.08.04, x.08.05, x.08.20	Multiple buffer overflow vulnerabilities and a faulty IP handling vulnerability exist in the firmware in the JetDirect card which could let a remote malicious user cause a Denial of Service.	Upgrade available at: http://www.hp.com/cposupport/networking/software/allhpjd3.exe.html	JetDirect Multiple Denial of Service Vulnerabilities	Low	Bug discussed in newsgroups and websites.
Krzysztof Dabrowski[17]	cmd5checkpw 0.20, 0.21	An authentication vulnerability exists which could allow a remote malicious user to send mail unauthenticated.	Upgrade available at: http://members.elysium.pl/brush/cmd5checkpw/	cmd5checkpw Qmail Remote Password Retrieval	Medium	Bug discussed in newsgroups and websites.
Mendel Cooper[18] Unix	Shred 1.0	A vulnerability exists in the way buffered I/O is processed which lets files remain recoverable by certain disk utilities.	The program's author notes: "I have 'officially' retired the package, will no longer distribute it, and e-mailed the Sunsite maintainers, asking them to remove it from their archive. This should resolve all remaining issues." ... "I therefore advise discontinuation of the use of the "shred" package. I have no plans to bugfix or update it, since Tom Vier's "wipe" package accomplishes the same job, and in a more thorough fashion."	Shred File Wiper Insecure File Deletion	Low	Bug discussed in newsgroups and websites.
Microsoft[19] Windows 95/98/NT 4.0/2000	Internet Explorer 4.x, 5.x prior to version 5.5	A security vulnerability exists which could enable a malicious user to obtain another user's userid and password to a web site.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq00-076.asp **Note:** The patch requires IE 5.01 SP1 to install. Customers who install this patch on other versions may receive a message reading "This update does not need to be installed on this system." This message is incorrect.	IE Cached Web Credentials	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[20] Windows NT 4.0/2000	Internet Information Server 4.0, 5.0	A directory traversal vulnerability exists which could potentially allow a malicious user to a web site to take a wide range of destructive actions against it, including executing arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq00-078.asp **Note:** The patch released with the advisory MS00-057 eliminates this vulnerability, therefore those who have already applied this patch do not have to take any further action.	IIS Web Server Folder Traversal	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.

[16] VIGILANTE Security Advisory, VIGILANTE-2000014, October 10, 2000.
[17] eSecurityOnline.com, October 17, 2000.
[18] Securiteam, October 14, 2000.
[19] Microsoft Security Bulletin, MS00-076, October 12, 2000.
[20] Microsoft Security Bulletin, MS00-078, October 17, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft[21] **Windows 95/98/NT 4.0/2000** ***Exploit script published[22]***	**Microsoft Outlook 97.0, 98, 2000; Internet Explorer 4.0 for Windows 3.1, 95, 98, NT 3.51, NT 4.0; Internet Explorer 5.0 for Windows 95, 98, NT 4.0, 2000, 5.01, 5.5**	**A vulnerability exists when viewing web pages or e-mail messages, which could allow a malicious user to execute arbitrary programs.**	**Unofficial Workaround (Georgi Guninski): Disable any active content in Internet Explorer or Outlook.**	**Internet Explorer / Outlook Express Com.ms.active X.Active XComponent Arbitrary Program Execution**	**High**	**Bug discussed in newsgroups and websites. Exploits have been published.** **Vulnerability has appeared in the Press and other public media.** ***New exploit script has been published.***
Microsoft[23] Windows 95/98/NT 4.0/2000	Microsoft Outlook Express 4.0, 5.0, 5.01, 5.5; Outlook 97, 98, 2000; Internet Explorer 4.0.1, 4.1, 5.0, 5.01, 5.5	A security vulnerability exists which could allow a malicious user to read local files, arbitrary URLs, and local directory structure after viewing a web page or reading a HTML message.	No workaround or patch available at time of publishing.	Microsoft IE / Outlook / Outlook Express Arbitrary Java Codebase Execution	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Microsoft[24] **Windows 95/98/NT 4.0/2000** ***New patch released[25]***	**Microsoft VM (2000 series, 3100-3300 series)**	**A security vulnerability exists when a user is visiting a malicious web site. The web site operator can masquerade as the user, visit other sites using his identity, and relay the information back to the attacker's site.**	***Frequently asked questions regarding this vulnerability and the patch can be found at:*** http://www.microsoft.com/technet/security/bulletin/fq00-075.asp ***Note: This fix supersedes the patch supplied in MS00-059.***	***Microsoft VM ActiveX Component***	Medium	**Bug discussed in newsgroups and websites.**
Microsoft[26] Windows NT 4.0/2000	NetMeeting Version 3.01 (4.4.3385)	A security vulnerability exists which could allow a malicious user to temporarily prevent an affected machine from providing any NetMeeting services and possibly consume 100% CPU.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq00-077.asp	NetMeeting Desktop Sharing	Low	Bug discussed in newsgroups and websites. Exploit has been published.

[21] Georgi Guninski Security Advisory #23, October 5, 2000.
[22] Securiteam, October 19, 2000.
[23] Georgi Guninski Security Advisory #24, October 18, 2000.
[24] Microsoft Security Bulletin, MS00-059, August 21, 2000.
[25] Microsoft Security Bulletin, MS00-075, October 12, 2000.
[26] Microsoft Security Bulletin, MS00-077, October 13, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft[27] **Windows ME/98/98SE** ***Patch available***[28]	**WebTV for Windows**	**Several Denial of Service vulnerabilities exist when a UDP packet is sent to any port in the 22701–22705 range.**	***Frequently asked questions regarding this vulnerability and the patch can be found at:*** http://www.microsoft.com/technet/security/bulletin/fq00-074.asp	**Microsoft WebTV Denial of Service**	**Low**	**Bug discussed in newsgroups and websites. Exploit has been published.** **Vulnerability has appeared in the Press and other public media.**
Microsoft[29] Windows 95/98/98se	Windows 95, 98, 98se	A Denial of Service vulnerability exists when a Windows 9x client tries to connect to File and Print sharing and the server returns an invalid driver type.	Microsoft recommends disabling the File and Printer Sharing component when a Windows 9x client tries to connect to the Internet using Dial-Up Networking. More information can be found at: Http://support.microsoft.com/support/kb/articles/Q199/3/46.ASP?LN=EN-US&SD=gn&FR=1	Windows 9x Invalid Driver Type Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[30] Windows 95/98/98se/ME	Windows 95, 98, 98se, ME	A Denial of Service vulnerability exists in the IPX NMPI (Name Management Port Interface) which could allow a remote malicious user to flood the network with superfluous data.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq00-073.asp	Windows 9x/ME Malformed IPX NMPI Packet	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[31] Windows 95/98/98se/ME	Windows 95, 98, 98se, ME	A security vulnerability exists which could allow a malicious user to programmatically access a Windows 9x/ME file share without knowing the entire password assigned to that share.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq00-072.asp	Windows 9x/ME Share Level Password	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Microsoft[32] Windows 98/9se/ME/NT 4.0/2000	Windows 98, 98SE, ME, 2000 (Hilgraeve Hyper Terminal 6.0 and previous)	A security vulnerability exists in the HyperTerminal application that ships with several Microsoft operating systems which could allow a malicious user to execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/fq00-079.asp	HyperTerminal Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[27] Bugtraq, September 12, 2000.
[28] Microsoft Security Bulletin, MS00-074, October 11, 2000.
[29] NSFOCUS Security Advisory, SA2000-03, October 11, 2000.
[30] Microsoft Security Bulletin, MS00-073, October 11, 2000.
[31] Microsoft Security Bulletin, MS00-072, October 10, 2000.
[32] Microsoft Security Bulletin, MS00-079, October 18, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Multiple Vendors[33] **Unix** ***Exploit script now available[34]***	**Lawrence Berkeley National Laboratory's traceroute 1.4a5; Debian 1.4A5-2; RedHat 6.0, 6.2; Caldera 2.4; Mandrake 7.0; Conectiva Linux 4.0, 4.0es, 4.1, 4.2, 5.0, 5.1; Solaris 2.5.1**	**A heap overflow vulnerability exists which could let local malicious users crash the application and possibly execute arbitrary code.**	**Contact your vendor for upgrade or patch.**	**Multiple Vendor Traceroute Heap Corruption**	**High**	**Bug discussed in newsgroups and websites. Exploit has been published.** ***Exploit script has been published.***
Multiple Vendors[35] Unix	OpenBSD 2.3-2.7; RedHat Linux 5.0, 5.1, 5.2 alpha, i386, sparc	A format string vulnerability exists which could allow a remote malicious user to execute arbitrary code, leading to a root compromise.	Contact your vender for patch.	BSD Talkd Remote Format String	**High**	Bug discussed in newsgroups and websites.
Multiple Vendors[36] Unix	PHP 3.00, 4.00	A format string vulnerability exists in the code that handles error logins, which could let a remote malicious user gain privileges of the webserver.	Upgrade available at: http://www.php3.org/downloads.php	PHP Error Logging Format String	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Multiple Vendors[37] Unix	SuSE Linux 6.4, RedHat Linux 6.1 (using the program cda); FreeBSD, OpenBSD (using the program /usr/bin/ systat); Caldera Linux	Several buffer overflow vulnerabilities exist in the screen handling library ncurses, which could let a malicious user elevate their privileges.	Contact your vendor for patch.	Ncurses Buffer Overflows	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[33] Securiteam, October 1, 2000.
[34] Bugtraq, October 6, 2000.
[35] Bugtraq, October 6, 2000.
[36] @stake Advisory, A 101200-1, October 12, 2000.
[37] Securiteam, October 19, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Multiple Vendors[38, 39, 40, 41, 42] Unix	RedHat Linux 6.2 alpha, i386, sparc, 7.0; Immunix OS 6.2; Mandrake 6.0, 6.1, 7.0, 7.1; Trustix Secure Linux (all versions); Conectiva Linux 4.0, 4.0es, 4.1, 4.2, 5.0, 5.1	A local Denial of Service and root exploit vulnerability exists which could let a malicious user execute arbitrary commands.	**RedHat:** ftp://updates.redhat.com **Immunix OS:** http://www.immunix.org:8080/ImmunixOS/6.2/updates/RPMS/tmpwatch-2.6.2-1.6.2_StackGuard.i386.rpm **Mandrake Linux:** ftp://ftp.linux.tucows.com/pub/distributions/Mandrake/Mandrake/updates **Trustix**: http://www.trustix.net/download/Trustix/updates/1.1/RPMS/ **Conectiva Linux:** ftp://atualizacoes.conectiva.com.br/	Tmpwatch Arbitrary Command Execution	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Netscape[43] Windows NT 4.0, Unix	Messaging Server 4.15, 4.15p1, 4.15p2	A vulnerability exists in the way e-mail addresses are verified which let a malicious user acquire a list of valid e-mail addresses.	No workaround or patch available at time of publishing.	Netscape Messaging Server E-mail Address Verification	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Netscape[44] Unix	Netscape iCal 2.1Patch2	Several vulnerabilities exist ranging from poor file permissions to insecure programming practices, which could allow local malicious users to obtain root access, and remote malicious users to monitor keystrokes.	A patch is available at: http://www.iplanet.com/downloads/patches/index.html	Netscape Multiple Vulnerabilities	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Nevis Systems[45] Windows NT 4.0/2000	All-Mail 1.1	Several buffer overflow vulnerabilities exist which could let a remote malicious user execute arbitrary code or a Denial of Service.	Nevis Systems is aware of this vulnerability but reportedly does not support the product anymore. Users are advised to use another mail package.	All-Mail Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Oatmeal Studios[46]	MailFile 1.10	A vulnerability exists in the Perl script, which could let a malicious site visitor have a given file dispatched to a specified e-mail address.	No workaround or patch available at time of publishing.	MailFile Arbitrary File Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[38] Red Hat, Inc. Security Advisory, RHSA-2000:080-01, October 6, 2000.
[39] Immunix OS Security Update, October 7, 2000.
[40] Linux-Mandrake Security Update Advisory, MDKSA-2000:056, October 7, 2000.
[41] Trustix Security Advisory, October 9, 2000.
[42] Conectiva Linux Security Announcement, October 9, 2000.
[43] Bugtraq, October 11, 2000.
[44] @stake, Inc. Security Advisory, A100900-1, October 9, 2000.
[45] @stake Inc. Security Advisory, A101200-2, October 12, 2000.
[46] Bugtraq, October 11, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
OpenBSD[47] Unix	OpenBSD 2.6, 2.7	An implementation vulnerability exists in the way xlock allows global variables in the initialized data section of memory to be overwritten, which could let a malicious user execute arbitrary code.	Patch available at: http://www.openbsd.org/errata26.html#xlockmore	OpenBSD Xlock Data overflow	High	Bug discussed in newsgroups and websites. Exploit script has been published.
PHPix[48]	PHPix 1.0-1.0.2	A directory traversal vulnerability exists which could let a malicious user read arbitrary files/folders.	No workaround or patch available at time of publishing.	PHPix Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
RedHat[49] Unix	Linux 6.2 alpha, i386, sparc, 7.0	Several buffer overflow vulnerabilities exist in ping: 1) Root privileges are dropped after acquiring a raw socket; 2) An 8 byte overflow of a static buffer "outpack" exists; and 3) An overflow of a static buffer "buf" exists.	Patch available at: ftp://updates.redhat.com	RedHat Linux Ping Buffer Overflow	Medium	Bug discussed in newsgroups and websites.
Stalker Software[50]	Communi Gate Pro 3.3.2	A vulnerability exists the Post Office Protocol Version 3 (POP3) daemon which could make it possible for e-mail address harvesters to populate lists with valid e-mail addresses, allowing the harvester to (for example) send spam to valid user accounts.	No workaround or patch available at time of publishing	CommuniGate Pro E-mail Address Verification	Low	Bug discussed in newsgroups and websites. Exploit has been published.
SuSE[51] Unix	Linux 6.2-6.4, 7.0	A format string vulnerability exists which could let a remote malicious user gain root access.	Upgrade available at: ftp://ftp.suse.com/pub/suse/	SuSE ypbind-mt Format String	**High**	Bug discussed in newsgroups and websites.
Valve Software[52] Unix	Half-Life Dedicated Server 3.1 and previous	A buffer overflow vulnerability exists in the changelevel rcon command, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Half-Life Dedicated Server	**High**	Bug discussed in newsgroups and websites.

[47] List Digest, October 10, 2000.
[48] Synnergy Laboratories Advisory SLA-2000-15, October 7, 2000.
[49] Red Hat, Inc. Security Advisory, RHSA-2000:087-02, October 18, 2000.
[50] Bugtraq, October 11, 2000.
[51] SuSE Security Announcement, uSE-SA:2000:042, October 18, 2000.
[52] Bugtraq, October 16, 2000.

Vendor/ Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
WQuinn[53] Windows NT 4.0/2000	QuotaAdvisor 4.1	A vulnerability exist in the directory listing disclosure which could allow unprivileged malicious users to obtain a complete list of files on the server.	No workaround or patch available at time of publishing.	QuotaAdvisor 4.1 Directory Listing Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
XFree86[54] Unix	Xlib 3.3x	A buffer overflow vulnerability exists in the DISPLAY environment variable, which could allow a malicious user to execute arbitrary code.	Upgrade to 4.0.x.	Xlib Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

*Risk is defined in the following manner:

High - A vulnerability that will allow an intruder to immediately gain privileged access (e.g., sysadmin, and root) to the system. An example of this would be a vulnerability in which a sequence of instructions is sent to a machine by an unauthorized user and the machine responds with a command prompt.

Medium - A vulnerability that will allow an intruder immediate access to the system that is not privileged access. This allows the intruder the opportunity to continue the attempt to gain root access. An example would be a configuration error that allows an intruder to capture the password file.

Low - A vulnerability that provides information to an intruder that could lead to further compromise attempts or a Denial-of-Service (DoS) attack. The reader should note that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered as a "High" threat.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between October 6 and October 21, 2000, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing**. During this period, 31 scripts, programs, and net-news messages containing holes or exploits were identified.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
October 21, 2000	Locale_sol.txt	Paper which describes in detail and contains the source code for the exploitation of the libc locale format string vulnerability on Solaris/SPARC.
October 21, 2000	Xzarch.c	Script which exploits the Linux /usr/games/zarch v.92 local root buffer overflow vulnerability.
October 20, 2000	Oracle-815.c	Script which exploits the Oracle 8.1.5 local buffer overflow vulnerability.

[53] Delphis Consulting Plc Security Team Advisories, DST2K0040, October 6, 2000.
[54] Securiteam, October 17, 2000.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
October 20, 2000	Pdump-0.782-2.tar.gz	A sniffer written in Perl, which dumps, greps, monitors, creates, and modifies traffic on a network. It combines features from tcpdump, tcpkill, ngrep, tcptrace, dsniff (and its webspy and urlsnarf), pfilt, macof, and xpy.
October 20, 2000	Sara-3.2.3.tar.gz	A security analysis tool based on the SATAN model.
October 20, 2000	Xsplumber.c	Script which exploits the Linux space plumber (/usr/games/splumber) local buffer overflow vulnerability.
October 18, 2000	**Guninski24.txt**	**Demonstration exploit for the Microsoft IE / Outlook / Outlook Express Arbitrary Java Codebase Execution vulnerability.**
October 18, 2000	Iisex.c	A remote command execution exploit for Microsoft IIS 4.0 and 5.0 Web Server Folder Traversal vulnerability.
October 18, 2000	Obtain-ics.sh	A proof of concept script which exploits Netscape iPlanet's iCal Multiple vulnerabilities.
October 18, 2000	Saint-3.0.1.beta1.tar.gz	A security assessment tool based on SATAN.
October 18, 2000	**Traceroute.c**	**Script which exploits the RedHat's Traceroute Heap Corruption vulnerability.**
October 17, 2000	Loit.c	Script which exploits the PHP Error Logging Format String for FreeBSD 3.4, Slackware Linux 4.0, and 7.0.
October 16, 2000	Wgate41a.c	Script which exploits the Wingate 4.1 Winsock Redirector Denial of Service vulnerability.
October 15, 2000	Ipchains-firewall-1.7.2.tar.gz	A configurable script to establish masquerading and firewalling rules using ipchains.
October 15, 2000	Sla-17.anaconda.txt	Exploit URL for Anaconda Foundation Directory Transversal vulnerability.
October 15, 2000	Snoopy-1.2.tar.gz	Snoopy is designed to log all commands executed by providing a transparent wrapper around calls to execve() via LD_PRELOAD.
October 12, 2000	**Allmailexp.c**	**Script which exploits the All-Mail Buffer Overflow vulnerability.**
October 12, 2000	Badphp.c	Script which exploits the PHP Error Logging Format String vulnerability.
October 11, 2000	Freebsd-systat.c	Exploit script for the FreeBSD 4.X local /usr/bin/systat vulnerability.
October 11, 2000	Saint-3.0.tar.gz	A security assessment tool based on SATAN.
October 10, 2000	Sla-16.masterindex.txt	Exploit URL for the Master Index for Linux/UNIX traversal vulnerability.
October 10, 2000	Xlockx.c	Script which exploits the OpenBSD xlock Data overflow vulnerability.
October 9, 2000	Boa.server.txt	Exploit URL for the Boa Webserver 0.94.2.x File Disclosure vulnerability.
October 9, 2000	Boa-httpd-exploit.pl	Perl script which exploits the Boa Webserver File Disclosure vulnerability.
October 9, 2000	**Shambala.pl**	**Perl script which exploits the Shambala Server Denial of Service and Plaintext Password Storage vulnerabilities.**
October 9, 2000	**Sla-15-phpix.txt**	**Exploit URL for the PHPix Directory Traversal vulnerability.**
October 8, 2000	**Godmessageiv.zip**	**An ActiveX exploit for Internet Explorer that attempts to install a Trojan on any machine which views the included HTML.**
October 8, 2000	Nmap-2.54beta7.tgz	A utility for port scanning large networks.
October 7, 2000	Tmpwatch.c	Script which exploits the Tmpwatch Arbitrary Command Execution vulnerability.
October 6, 2000	Fwsa.sh	A tool to penetration test Checkpoint Firewall-1 remotely which implements recently published holes in session authentication. It attempts to recover user passwords, execute DoS attacks, and brute force the firewall management password.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
October 6, 2000	Hert.0003.freebsd.isn	Proof of concept code for the FreeBSD random sequence number vulnerability.

Script Analysis

When available, this section will supply a short description of scripts that have been analyzed by various security professionals and organizations. **We encourage you or your organization to contribute.** If you wish to do so, please send e-mail to nipc@fbi.gov with the subject line "CyberNotes Script Analysis." While space constraints may limit the length of descriptions included in this document, contributors are requested to include a full technical analysis of the script along with release instructions. The release categories are: releasable to anyone; limited releasability (originator-defined list of organizations); or provided for NIPC only. A member of the CyberNotes editorial team will contact you. All contributions will be credited to the contributing individual or organization unless otherwise requested.

No scripts were submitted during the two-week period covered by this issue of CyberNotes.

Trends

DDoS/DoS:

A new variant of the SubSeven Trojan Horse has been discovered in the wild. For more information please see NIPC ADVISORY 00-056 located at:
http://www.nipc.gov/warnings/advisories/2000/00-056.htm.
New Variants of the Trinity and Stacheldraht Distributed Denial of Service tools have been reported in the wild. The new versions of Stacheldraht include "Stacheldraht 1.666+antigl+yps" and "Stacheldraht 1.666+smurf+yps," and the new version of Trinity is "entitee." For more information please see NIPC ADVISORY 00-055 located at:
http://www.nipc.gov/warnings/advisories/2000/00-055.htm**.**
Numerous sites that still run an old version of Apache have been victimized by a Windows-based DDoS attack originating from over 500 different IP addresses.
A steady number of reports of intruders using nameservers to execute packet-flooding Denial of Service attacks.

Probes/Scans:

Intruders are using scripts and toolkits to automate attacks against the input validation problem in rpc.statd and the input validation problems in FTPD, the site exec vulnerability. For more information see CERT advisory located at: http://www.cert.org/incident_notes/IN-2000-10.html.
Intruders are actively exploiting a vulnerability in telnetd that is resulting in a remote root compromise of victim machines.

Other:

Directory Traversal vulnerabilities have appeared in numerous web shopper software packages.
Even though TROJ_SKA and VBS_KAKWORM.A were found several months ago, they continue to spread and infect new users.
Multiple vulnerabilities have been published concerning OpenBSD.
The CERT Coordination Center has issued a new policy with respect to the disclosure of vulnerability information. For more information please see advisory at:
http://www.cert.org/faq/vuldisclosurepolicy.html.
Mobile Operating Systems have become the latest target of virus writers and hackers.

Viruses

A list of viruses infecting two or more sites as reported to various anti-virus vendors has been categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication**. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available**. The tables list the viruses by: ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported during the latest three months), and approximate date first found. During this month, a number of anti-virus vendors have included information on Trojan Horses and Worms. These types of malicious code will now be included in the table where appropriate. Following this table are write-ups of new viruses and updated versions discovered in the last two weeks. WARNING: at times, viruses may contain names or content that may be considered offensive.

Note: Virus reporting may be weeks behind the first discovery of infection. A total of **214** distinct viruses are currently considered "in the wild" by anti-virus experts, with another **583** viruses suspected. "In the wild" viruses have been reported to anti-virus vendors by their clients and have infected user machines. The additional suspected number is derived from reports by a single source. **Editor's Note: The October 2000 virus table demonstrates a significant increase in the number of Trojans being reported in virus frequency tables.**

Ranking	Common Name	Type of Code	Trends	Date
1	VBS/LoveLetter	Script	Increase	March 2000
2	VBS/Kakworm	Script	Slight decrease	December 1999
3	PE_MTX.A	File Infector, Trojan	New to table	September 2000
4	VBS/Stages	Script	Slight increase	June 2000
5	W97M/Ethan.A	Macro	Increase	February 1999
6	Qaz.A	Trojan	New to table	August 2000
7	W32/SKA	File	Decrease	March 1999
8	W97M/Marker	Macro	Decrease	August 1998
9	FunLove	File	New to table	November 1999
10	SubSeven	Trojan	Stable	March 2000

PE_DENGUE (Aliases: DENGUE, W32.Dengue, Win32.CTX.10853, Win32.CTX.6886 (Polymorphic Virus): This is a memory resident polymorphic Win32 virus which infects EXE, SCR, and CPL in the subdirectories of all local hard drives. It also deletes several antivirus checksum files.

JS/VBS.LostSoul.Worm (Visual Basic Script Worm): This worm spreads via e-mail. When executed, it displays a text file containing the Wobbler Hoax. The attachment in the e-mail message is named Wobbler.txt.jse or Wobbler.txt.vbe. When opened, these attachments create and execute a temporary file containing malicious code. The worm also spreads via networks by copying itself to the root directories of shared drives. The worm originated in Argentina.

VBS/CoolNotepad.Worm: (Visual Basic Script Worm): This virus is transmitted by IRC and Microsoft Outlook. When the file COOL_NOTEPAD_DEMO.TXT.vbs (which comes as an e-mail attachment or via an active IRC channel) is executed, the virus copies this file to the Windows SYSTEM directory. VBS/CoolNotepad.Worm makes certain entries in the Windows registry to ensure its execution every time the system is started or rebooted and hide the desktop at the same time. The virus also creates an e-mail message, which will be sent to all contacts in the address book.

VBS/Godzilla@M (Visual Basic Script Worm): This worm functions the same way that JS/Kak.worm does. Like JS/Kak.worm, a dangerous aspect of this Internet worm is its ability to continuously re-infect yourself. This worm uses VBScript and an ActiveX component, called "Scriptlet Typelib," to propagate itself through e-mail using MS Outlook Express. When an e-mail or newsgroup message infected by this worm is opened by a reader who supports VBScript in HTML, it writes the Update.hta file to the Startup folder of the local machine. This will launch the code embedded in the HTA file at the next Windows startup. ***Microsoft has published a security update, which addresses this ActiveX exploit, and users are encouraged to update their systems with this component***.

VBS/Kakworm-D (Aliases: Mid/Kakworm-D) (Visual Basic Script Worm): This is a variant of VBS/Kakworm which only affects users of Microsoft Outlook Express 5 running under French Windows. If the user opens or previews an infected e-mail message, the worm will drop TAM.HTA to the Windows start-up folder. It also creates C:\WINDOWS\OUT.HTML, which then sets as the default signature of Microsoft Outlook Express, so that it gets attached to all outgoing e-mail messages. The worm will be reported as Mid/Kakworm-D if it is detected in an e-mail.

VBS/LoveLet-BI (Visual Basic Script Worm): This is a variant of the VBS/LoveLet-A worm (also known as The Love Bug). The worm arrives in the form of an e-mail attachment and if launched forwards itself to addresses in your Outlook address book. The e-mail has the following characteristics:

Subject: Gotov je! 24.09.2000!
Text: Ej! Pogledaj ovo u prilogu!!!
Attachment: GotovJe.vbs

The worm writes different copies of itself to the Windows directory and the Windows\System directory. The worm then displays an HTML file, which says:

KOMSIJA,
24 Septembra su izbori! Na time izborima TI pobedjujes
Milosevica! Tvoj glas ga plasi!
24.09 Izadji, Glasaj, Pobedi!
Gotov je!

VBS.Plan.D (Visual Basic Script Worm): This is a variant of the VBS.Plan worm. The worm spreads via Microsoft Outlook. When executed, the worm copies itself into:

Windows directory as Reload.vbs
Windows\System directory as Linux32.vbs
Windows\System directory as a randomly generated four to eight character file ending in .gif.vbs, .jpg.vbs, or .bmp.vbs

The worm ensures execution upon Windows startup by setting two keys in the Windows registry, the Run key and the RunServices key. The worm also checks to see if there is a default download directory set for Microsoft Internet Explorer. If not, it sets C:\ as the default download directory. The worm creates a file named Us-president-and-fbi-secrets.htm in the Windows directory, but this file does not get loaded. The worm uses MAPI to call to Microsoft Outlook, and creates messages by iterating through all the addresses in the Outlook address book. The worm marks the recipients using the registry and attempts to send them mail only once. The randomly generated file names that the worm creates appear in all capital letters and are formatted so that every even numbered letter is a vowel, for example, SOXU, DEII, YIEUHUDI, BILALU, and so on.

VBS.Tam.A (Aliases: VBS.Out, VBS/Out@M) (Visual Basic Script Worm): This is a worm which utilizes a known Microsoft Outlook Express vulnerability called Scriptlet.Typelib so that a viral file is created on the system without having to run an attachment. Simply reading or previewing an e-mail message with the worm attached causes the worm to be placed on the system. Upon execution, the worm inserts a copy of itself into the StartUp directory of the Windows operating system. However, this only works if the operating system is French. The worm creates a file named Tam.hta. On the 30th of August, the worm displays a dialog box on infected systems, containing the following text:

"Bon Anniversaire Lac
Un ami..."

W32.HLLW.Bymer (Internet Worm): This is a worm written in a high level language. The worm spreads via shared network drives. It looks for shared folders on the network, and copies itself if it is able to insert itself in the Windows\System folder. The payload includes copying the Dnetc client and modifying the Win.ini file. The Dnet client is not viral and will not be detected by Norton antivirus. The worm was previously detected as Dnet.Dropper.

W97M.Celebrate.A (Word 97 Macro Virus): W97M.Celebrate.A conceals its presence by turning off the VirusProtection option, the ShowVisualBasicEditor option, and by deleting the Macro selection in the Tools menu. The virus is activated on AutoOpen, AutoClose, New Document, and Document Open. On AutoClose, C:\Windows\Command\Qbasic.exe is copied to A:\~Wd01106.doc. The virus then attempts to infect the Normal template and all active documents. The virus checks to see if Qbasic.exe is on the infected machine. If the file does not exist, the virus attempts to create it by copying A:\~Wd01106.doc to C:\Windows\Command\Qbasic.exe. Finally, the virus checks the date. If it is the 11th of the month, the payload is executed. The payload consists of the following actions:

Copy C:\Autoexec.bat to C:\Csp_c_au.bat,
Modify C:\Autoexec.bat so that the next time the infected computer starts, some messages are displayed in Spanish.

Some parts of the payload will not work properly if Qbasic.exe is not on the infected computer.

W97M.Cheechoong.A (Word 97 Macro Virus): This is a very small macro virus that replicates using the Normal.dot template file. If the current day of the month is equal to the number of the current month, the Office Assistant displays a message. The virus activates on document open. The virus first conceals its presence by switching off VirusProtection, SaveNormalPrompt, and ConfirmConversions. It then attempts to infect the Normal.dot template file and the active document. The payload is executed if the current day of the month is equal to the number of the current month. The Office Assistant appears with the following message: "Have a great CheeChoong..."

W97M.Invert.A (Alias: Karachi_y2k) (Word 97 Macro Virus): The virus activates on Document Open, Document Close, and New Document. W97M.Invert.A first turns off the VirusProtection option in order to remain undetected. The virus then infects the Normal.dot template and all active documents. The following payload is executed if the current day of the month is divisible by two. n all of the following files, bytes four through 1020 are inverted:

C:\Windows\System\Netcpl.cpl
C:\Windows\System\Inetcpl.cpl
C:\Windows\System\Modem.cpl
C:\Windows\Sol.exe
C:\Windows\Mshearts.exe
C:\Windows\Freecell.exe
All files on the C drive with the extension .MD?

If the current day of the month is divisible by four, bytes four through 1020 of the following files are also inverted:

C:\Windows\System\Msprint.dll
C:\Windows\System\Msprint2.dll

If the current day of the month is divisible by six, any instance of LPT in C:\Windows\Win.ini is replaced with LPD.

W97M/Marker.CW (Word 97 Macro Virus): W97M/Marker.CW is activated on certain dates and on each of these, carries out different actions. On the 15th of February, April, June, August, October or December it deletes all text in the infected document and on the 13th of any month it changes the document font to Webdings. The virus also disables the macro virus protection so that the user cannot enable or disable macros defined in Word documents.

W97M/PassBox.I (Word 97 Macro Virus): This virus is capable of stealing document passwords from Word documents. To do this it prompts the user to enter passwords into a dialog box similar to those used by Word. Once it has obtained a password it stores it in a file called MSDOS.SDX in the root directory of the hard disk. The virus also disables the macro virus protection so that the user cannot enable or disable macros defined in Word documents.

W97M_ PassBox.Q (Aliases: PASSBOX, W97M_Passbox.q.gen, W97M.DWMVCK1/ZMK, Macro.Word97.Passbox.a) (Word 97 Macro Virus): This macro virus infects MS Word documents and document templates. If the current system weekday number is equal to a random number (1 to 7) generated by the virus, an animated string is inserted at the start of the document. The office assistant balloon also displays some text.

W97M_PENE.C (Aliases: PENE.C, Macro.Word97.Free) (Word 97 Macro Virus): This polymorphic MS Word 97 macro virus infects Word documents and the global template. It hides its virus code when viewed in the Visual Basic Application window.

W97M/Seliuq (Word 97 Macro Virus): This is a macro virus, which infects documents in Microsoft Word 97 and the NORMAL.DOT global template that this uses as a base for all documents. The virus creates a file called SYSTEMDOS in the root directory of the C: drive. This file contains a log in which it stores the names of all the directories it has infected. When the file SYSTEMDOS reaches a size of 1024 Bytes, W97M/Seliuq attempts to activate its payload. Due to an error, however, it is not capable of carrying out its destructive task.

W97M_SHORE.D (Aliases: SHORE.D, Macro.Word97.Shore) (Word 97 Macro Virus): This macro virus deletes all user macros contained in the document. When the Visual Basic Editor is accessed, an input box is displayed. If the infected user types in the wrong password, and then presses the "OK" button, an error message box is displayed. If the user types in the correct password, the Visual Basic editor window is displayed.

WM97/Class-EZ (Word 97 Macro Virus): This is a variant of the WM97/Class Word macro virus that has been reported in the wild.

WM97/Marker-FP (Word 97 Macro Virus): This is a variant of the WM97/Marker Word macro virus. This virus changes the Word Application Username to "JonMMx2000," the user initials to "MeMeX" and the user address to "JonMMx2000@yahoo.com." On Mondays, it will create the file jon.html in the directory in which Windows is installed.

WM97/Metys-I (Word 97 Macro Virus): On September 18th the virus displays a message box:

> "Happy Birthday Jess! To celebrate, we're going to see how lucky
> you are <Username>. Click the OK button below to roll a number.
> If your number matches that of the dealer, you win!"

If you win the virus displays the message:

> "You roll a <number between 1 and 9> and the dealer rolls a
> <same number between 1 and 9>. You win!"

If you lose the virus displays the message:

> "You roll a <number between 1 and 9> and the dealer rolls a
> <number between 1 and 9>. I'm sorry, but you lost. Better luck
> next time!"

WM97/Thus-BO (Word 97 Macro Virus): This is a variant of WM97/Thus-AM Word macro virus, but the payload has been removed.

WM97/Titch-G (Word 97 Macro Virus): This virus is a variant of the WM97/Titch virus. It a simple Word macro virus. The virus code includes the following text, which does not get displayed:

> "If you had looked you could have found and deleted it but.. You probably never knew it was here!"

WM97/Title-A (Word 97 Macro Virus): On 3 May, 20 June and 30 July this virus will password protect the infected document. The password is a randomly chosen integer between -1 and 9.

X97M_Barisada.H (Aliases: BARISADA.H, X97M/Barisada.gen, Macro.Excel97.Barisada.C, X97M/Barisada.E) (Excel 97 Macro Virus): This virus infects activated and deactivated workbooks. Selected cells in the active workbook are cleared when user clicks on the wrong button when prompt by the virus. If the current system date is April 24 and the time is 2.xx PM, the virus displays several message boxes.

XM97/Barisada-J (Excel 97 Macro Virus): This is a variant of the XM97/Barisada-A Excel macro virus. The viral macros are stored in the file HJB.XLS. On 24 April between 2pm and 3pm, the virus displays a series of dialog boxes asking the user questions which may be related to a fantasy role playing game. The first dialog box has the title '1st Question' and the text 'Question : What is the Sword Which Karl Styner(=Grey Scavenger) used? Answer: Barisada'. If you press 'No' a dialog box with the title 'Right Answer' and the message 'Good! You're Authorized now!!' is displayed. If you press 'Yes' then a dialog box with the title 'Wrong Answer' and the text 'I will give you one more Chance. Be careful!!' is displayed. The next dialog box has the title 'Wrong Answer may cause The Serious Problem!' and the text 'Summoning Xavier is the Ultimate Magic. Right?'. If you press 'Yes' a dialog box with the title 'Right Answer' and the message 'ok , I will forgive you' appears. If you press 'No' a dialog box with the title 'You shall Die' and the message 'Wrong Answer, Your file will be deleted!' appears. The virus then clears all the cells in all the open sheets.

X97M.Threekay.A (Excel 97 Macro Virus): This virus infects workbooks by inserting an infected sheet named Book1 in the Microsoft Excel Start directory. The virus also attempts to switch off virus protection by inserting two files: C:\Tb6.bat and C:\Tb6.reg. The virus then iterates through the active workbooks and check for macros inside them. If the number of lines of code found exceeds 3000, the iteration is halted and the virus continues with the next section. If there are not more than 3000 lines of code, no action is taken. After the first iteration, the file Book1 is inserted in the Excel Start directory to make sure that any newly opened files become infected. The virus then starts a second iteration through all workbooks and macros. During this second iteration any uninfected files are infected. The payload is executed when the current day of the month is equal to the current minute.

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. The increasing number of Trojans gains added significance due to recent testing conducted to determine the ability of anti-virus software to detect Trojans. According to the test results, a number of popular anti-virus products failed to detect or had limited detection capabilities against current popular Trojans. Testing also indicates that detection of a baseline Trojan does not necessarily mean the anti-virus software can detect a variant. Readers should contact their anti-virus vendors to obtain specific information on Trojans and their variants that their software detects.

The following table provides the reader with a list of Trojans that have received write-ups in CyberNotes. This table includes Trojans discussed in the last six months and will be updated on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. NOTE: At times, Trojans may contain names or content that may be considered offensive.

Trojan	Version	Issue discussed
Asylum + Mini	v0.1, 0.1.1, 0.1.2, 0.1.3 + 1.0, 1.1	CyberNotes-2000-10, CyberNotes 2000-12
AttackFTP		CyberNotes-2000-10
Backdoor/Doly.17		CyberNotes-2000-16
BackDoor-GZ		CyberNotes-2000-18
BackDoor-HC		CyberNotes-2000-18
Backdoor-HD		CyberNotes-2000-18
BF Evolution	v5.3.12	CyberNotes-2000-10
BioNet	v0.84 - 0.92 +2.2.1	CyberNotes-2000-09, CyberNotes 2000-12
Bla	1.0-5.02, v1.0-5.03	CyberNotes 2000-09
Bobo	v1.0 - 2.0	CyberNotes-2000-09
Donald Dick 2		CyberNotes-2000-15
Drat	v1.0 - 3.0b	CyberNotes-2000-09
Erap Estrada		CyberNotes-2000-18
GIP		CyberNotes-2000-11
Golden Retreiver	v1.1b	CyberNotes-2000-10
Hooker-E		CyberNotes-2000-19
ICQ PWS		CyberNotes-2000-11
InCommand	1.0-1.4, 1.5	CyberNotes-2000-09
Infector	v1.0 - 1.42, v1.3	CyberNotes-2000-09
iniKiller	v1.2 - 3.2, 3.2 Pro	CyberNotes-2000-09, CyberNotes-2000-10
Kaos	v1.1 - 1.3	CyberNotes-2000-10
Khe Sanh	v2.0	CyberNotes-2000-10
Magic Horse		CyberNotes-2000-10
Matrix	1.4-2.0, 1.0-2.0	CyberNotes-2000-09
Mosaic	v2.00	CyberNotes-2000-16
Multijoke.B		CyberNotes-2000-15
Naebi	v2.12 - 2.39, v2.40	CyberNotes-2000-09, CyberNotes 2000-12
Netbus.153		CyberNotes 2000-16
Netbus.170		CyberNotes 2000-16
NetSphere	v1.0 - 1.31337	CyberNotes-2000-09
Netsphere.Final		CyberNotes-2000-15
NoDesk		CyberNotes-2000-14
Omega		CyberNotes 2000-12
Palm/Liberty-A		CyberNotes-2000-18
PALM_VAPOR.A		CyberNotes-2000-19
PE_MTX.A		CyberNotes-2000-18
Phaze Zero	v1.0b + 1.1	CyberNotes-2000-09
Prayer	v1.2 - 1.5	CyberNotes-2000-09
Prosiak	beta - 0.65 – 0.70 b5	CyberNotes-2000-09, CyberNotes 2000-12
Qaz.A	W32.HLLW.Qaz.A	CyberNotes-2000-20, CyberNotes-2000-16
Revenger	1.0-1.5	CyberNotes 2000-12

Trojan	Version	Issue discussed
Serbian Badman		CyberNotes 2000-12
ShitHeap		CyberNotes-2000-09
Snid	1-2	CyberNotes 2000-12
Troj/Simpsons		CyberNotes-2000-13
TROJ_BATMAN		CyberNotes-2000-20
TROJ_BLOODLUST		**Current Issue**
TROJ_BUTANO.KILL		CyberNotes-2000-19
Troj_Dilber		CyberNotes-2000-14
TROJ_IGMNUKE		CyberNotes-2000-20
TROJ_KILLME		CyberNotes-2000-20
TROJ_MSINIT.A		**Current Issue**
TROJ_PERSONAL_ID		CyberNotes 2000-16
TROJ_POKEY.A		CyberNotes 2000-16
TROJ_SCOOTER		CyberNotes-2000-19
TROJ_SPAWNMAIL.A		CyberNotes-2000-18
TROJ_SUB7.214DC8		**Current Issue**
TROJ_SUB7.382883		**Current Issue**
TROJ_VBSWG		CyberNotes-2000-16
Trojan/ICQ		CyberNotes-2000-20
Trojan/Parkinson		**Current Issue**
Trojan/PSW.StealthD		CyberNotes-2000-19
Trojan/Varo31		CyberNotes-2000-19
Trojan/Win32		**Current Issue**
W32.Nuker.C		CyberNotes-2000-14
Win.Unabomber		CyberNotes-2000-14
WinCrash	Beta	CyberNotes-2000-12
Winkiller		CyberNotes 2000-12

TROJ_BLOODLUST: This nonpolymorphic, nonmemory-resident Trojan program causes networked computers to disconnect from the network or crash.

TROJ_MSINIT.A (Aliases MSINIT.A, W32/Msinit): This Trojan was recently reported in the wild. Once executed, this Trojan modifies the registry so that it is executed every time the system is started. It also attempts to spread itself to other computers by scanning IP addresses over NetBIOS. It searches for computers with a shared C:\ drive, which also contains the "Windows" directory. On an infected system, TROJ_MSINIT.A runs the file "DNETC.EXE," an encryption cracking program.

TROJ_SUB7.214DC8 (Aliases: SUB7.214DC8): This Trojan program allows a remote user to access the infected PC. It contains two parts: the client part, which runs remotely; and the server part, which runs on the infected computer. Once the client part of the Trojan connects with the server part, the remote user running the client part can control the infected PC.

TROJ_SUB7.382883 (Aliases: SUB7.382883, BACKDOOR): This Win32 Trojan is a new member of the SubSeven families of backdoor Trojans. This variant differs from others due to its mode of installation on the infected computer, and server. The Trojan is the server side of the hacking tool, which enables a remote user to gain access to the infected computer. It also copies itself and modifies Windows initialization files, so that the Trojan is run after the Windows start up. This Trojan is like the Back Orifice Trojan and compromises security network, since it gives administrator privileges to a remote user via the Internet.

Trojan/Parkinson: This is a Trojan that adopts the aspect of the installation of a game called Sextris or Sexgame. After requesting users to enter their names and surnames, it creates files 'VIRUS.BAT' and 'MAJO.COM' in the TEMP directory. When the VIRUS.BAT file runs, it deletes the boot files (IO.SYS, MSDOS.SYS, COMMAND.COM, CONFIG.SYS, AUTOEXEC.BAT) and other files from the Windows and COMMAND directory. When Trojan/Parkinson has finished its destructive tasks, a dialog box appears with a photo of the supposed author of the virus.

Trojan/Win32: This is a Trojan that facilitates Denial of Service attacks by sending ICMP packets en masse to a certain IP address. The attacks have two objectives: to crash the target machine, and to close the current connection with the Internet or the IRC channels.